# Enhancing IoV Integration: The Critical Role of Secure Data Transmission in IoT and Electric Vehicle Ecosystems

Faisal Faisal
College of Graduate Studies
University Tenaga Nasional, Malaysia
Faisal.hadi.it@gmail.com

Moamin Mahmoud
College of Computing and Informatics
University Tenaga Nasional, Malaysia
moamin@uniten.edu.my

Abba Hassan
College of Graduate Studies
University Tenaga Nasional, Malaysia
zumkas@yahoo.com

Salama Mostafa
Department of Artificial Intelligence Engineering Techniques, Alnoor University, Iraq
salama.adress@alnoor.edu.iq

Saraswathy Gunasekaran
College of Computing and Informatics, University Tenaga Nasional, Malaysia
sshamini@uniten.edu.my

**Abstract:** *Efficient data transmission within this ecosystem is critical as integrating the Internet of Things (IoT) and Electric Vehicles (EVs) becomes increasingly common. This study examines the crucial role of data transmission in Internet of Vehicles (IoV) integration through a systematic literature review to clarify how EVs integrate into the larger IoT ecosystem and how data transmission performs a crucial role in enabling efficient interaction. It employed the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) methodological framework to analyze existing data transfer protocols and their performance in real-world applications. It summarizes existing research and provides a roadmap for future directions, addressing unresolved data transmission and security challenges in IoV systems. The review addressed four essential questions related to the types and properties of data transmitted between EVs and their impact on IoT in the context of IoV improvement. Furthermore, an evaluation systematically analyses and assesses risks related to transmitting information in the environment of EVs, considering any potential difficulties or weaknesses. To address these challenges, we propose a Hybrid Blockchain-Based (HBB) model for addressing these challenges, combining edge computing with lightweight, conventional blockchain architectures to ensure secure, scalable, and immediate data transmission. Through extending on previous implementations in EV networks, our method improves data quality and resilience while using the advantages of both blockchain types of lightweight for edge efficiency and standard for strong security and immutability. The review emphasizes the importance of reliable data transfer protocols to maximize EVs' performance, efficiency, and overall IoT integration. Comprehending these risks is essential for developing resilient and secure communication protocols in the IoV convergence. The finding emphasizes the significance of resolving data transmission issues to fully realize the opportunity of EVs on the IoT.*

**Keywords:** *Internet of things, electric vehicles, internet of vehicles, security, data protection, blockchain, smart grid.*

*Received January 22, 2025; accepted June 1, 2025*
*https://doi.org/10.34028/iajit/22/5/4*

## 1. Introduction

The rapid growth of technology has immersed us in a digital landscape where safeguarding data privacy and security from a myriad of threats is a paramount concern [34]. Electric Vehicles (EVs) are, therefore, progressively dependent on Internet of Things (IoT) in real-time communication with charging infrastructure, traffic management systems, and other smart grid systems. This means that when IoT devices collect and facilitate easy transmission of sensitive data, unauthorized access and manipulation create cyber-attacks, among others [15]. These risks, therefore, seriously call for advanced solutions. In essence, blockchain technology has proved to be one approach with high prospects of enhancing the Internet of Vehicles (IoV) ecosystem's data security, scalability, and privacy.

One of the main drivers encouraging IoT growth in the EV ecosystem is the affordability of hardware, services, and management infrastructures. However, centralized systems face security concerns when IoT is widely deployed in EV networks. These systems are susceptible to single points of failure since they depend on costly servers and infrastructure. A central server that stores EV and charging session data might be compromised by attacks like Distributed Denial-of-Service (DDoS), which would cause major service interruptions. This vulnerability between multiple entities of such IoV systems enforces revisiting current organizational structures and further investigating decentralized approaches like blockchain technology, which offers better security and resilience for the overall system [16].

The IoV integration has enhanced operational efficiency and improved the user experience. Being a connected framework, it gives efficient communication

among EVs and other internal systems, including charging stations, traffic management, and other smart devices, through the consistent transmission of real-time data. For example, data communication between the EVs and charging infrastructure should be continuous in nature to support optimized charging times, route planning, and energy use with a general view towards better performance and satisfaction. Connectivity can indeed change how efficient and convenient the EVs have become; however, it also brings along very critical concerns regarding data transmission security, reliability, and efficiency. Large volumes of critical information, such as location, driving behavior, and energy usage, are collected and transmitted, requiring significant security measures against unauthorized access and data alteration. Under increasing IoV ecosystems, risks must be drawn with their appropriate and effective countermeasures to sustain benefits from this integration [23].

Users would soon be living and doing almost everything through their EVs, generating a huge amount of sensitive information about their location, driving preferences, status of the vehicle, etc. In both cases, the data should be well-protected throughout their lifecycle from transmission to storage to prevent unauthorized access or cyber-attacks [44]. To mitigate those risks, in EVs, different security techniques, which include encryption, authentication, and remote monitoring among others, are applied by IoT systems through multilayer defense against cyber threats [1]. The assurance of data confidentiality, integrity, availability, and authentication of sensitive EV data is what all the layers are directed toward [27].

The study proposes a cloud-edge hybrid architecture to overcome issues with data transmission and security in the IoV The system can improve reaction times and lower latency by using edge devices for local data processing. Furthermore, blockchain-based solutions enhance data security and scalability, especially energy-efficient consensus techniques like Proof of Stake (PoS) and off-chain data storage. To improve privacy while preserving transparency, the study also investigates homomorphic encryption and zero-knowledge proofs, which will eventually improve IoV security and smart grid network performance. Thus, this study aims to investigate the critical aspects of data transmission in an IoV integrated framework. Examining prior literature and technological advancements, the study seeks to identify the current challenges, highlight effective solutions, and propose future research directions. Focusing on data transmission protocols and security frameworks will study the possibility of enhancing the current architecture of data security and integrity through emerging technologies such as blockchain in IoV networks. Therefore, the following are the research questions that guide the study. The following research questions are formulated to guide the investigation and give a clear direction toward addressing the most pressing issues surrounding IoV data transmission and security.

- **RQ1:** How are different types of data transmitted between EVs?
- **RQ2:** What are the privacy risks associated with the transmission of EV data?
- **RQ3:** What are the existing techniques for protecting the privacy of transmitted EV data?
- **RQ4:** What challenges are encountered in storing, gathering, and transmitting data within EVs?

The remainder of this study is structured into the following sections. Section 2 reviews previous literature and describes what is currently known about data transmission protocols and security measures in the context of IoV integration. Section 3 explains Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) framework approach which is used for systematic review-including study selection criteria and data extraction method. In section 4, present findings from our review with emphasis on performance evaluation as well as security analysis for different types of existing protocols. Section 5 addresses the findings, its implications, and identified challenges. Finally, section 6 presents the study conclusion by summarizing key findings and recommendations.

## 2. Related Work

This section reviews the existing literature, categorizing it into four primary areas: Data transmission, security challenges, blockchain technology, and EV.

### 2.1. Data Transmission

IoT data transmission is the process of collecting and converting data gathered by connected devices into useful information for the user, Said [34]. This process is crucial for advancements in various domains, such as smart grids, EVs, and Cyber-Physical Systems (CPS). The study carried out an extensive analysis of information and communication technologies in contemporary Demand-Side Management (DSM) for smart grids, with a focus on privacy, cybersecurity, sustainability, and resilience. It looked at M-Bus for electric meter integration, wireless connectivity, Modbus (Ethernet Transmission Control Protocol (TCP)/IP/RS232/RS485), and multicast packets, among other DSM communication methods. The study emphasized the necessity of inclusive management techniques to increase grid stability while reducing customer annoyance and recommended future lines of inquiry for cybersecurity and data analysis research to advance DSM [34].

Similarly, this study and communication technologies for EV adoption, emphasizing important protocols including Open Charge Point Protocol (OCPP), OpenADR, and eMIP as well as machine learning for predictive analytics. Although charging, billing, and grid management are supported by these protocols, scalability and security challenges continue. Obstacles include

juggling interoperability, security, and efficiency as well as privacy issues and large data infrastructure. Blockchain has energy and scalability issues despite its security advantages. To integrate EVs into IoT-driven smart grids, several problems must be resolved [27].

The work of studied power-electronic developments in CPS, with an emphasis on how power electronics might be integrated with communication technologies to share data in real time. Despite being essential to the dependability of the smart grid, CPS are vulnerable to cybersecurity threats and possible malfunctions that might result in cascade failures. To safeguard CPS, fault-tolerant communication methods and cybersecurity must be strengthened. To guarantee reliable smart grids, the study emphasizes the necessity for more research on safe communication and security measures [10].

Primary features like metering, communication, and cloud computing were highlighted in a review of smart grid technology, with an emphasis on the financial advantages of resource management and energy saving. High investment costs, standard problems, Supervisory Control and Data Acquisition (SCADA) system constraints, and security considerations are obstacles, nevertheless. Strong, interoperable infrastructure is necessary for efficient data transfer, but it is expensive and complicated. Furthermore, operational efficiency is impacted by poor SCADA response rates, which impede real-time data transmission [7].

The survey of further identified that barriers to interoperability between legacy and newer technologies due to integration problems hinder adoption. Yet another major factor underlying it was constraints of the utilities by SCADA systems in terms of response times not capable of enabling real-time data exchange for ideal grid operations. The review accentuated that the infrastructure must be robust, interoperable, and able to handle effective and secure data communication. Such an infrastructure could be very expensive to implement. There are gaps in standardization and integration issues that could lead to inefficiencies and loss of data, as well as bottlenecks in operations that dent the functionality of smart grids. Besides, the study underlined major cybersecurity threats that might lead to protection in data transmission as a way of further mitigating the threats to maintain the integrity and security of the smart grid systems [22].

The study of addressed the intricacy of these interactions by proposing a four-layered architecture for energy trading to facilitate communication and data exchange between different parts of the grid, making it more detailed. The study also provided a comprehensive problem taxonomy for energy trading challenges. It introduced causal links between these problems, which were extended into mechanisms allowing us to follow potential entries for solution pathways, such as demand forecasting improvement, flexibility in the grid system, and secure/efficient trading of electricity. Despite these, the study highlighted future research challenges in smart grid energy trading technically, economically, and socially, which needs continuous endeavors despite optimistic progress [44].

These underscore the importance of effective data transmission technologies in developing and managing modern smart grids, EVs, and CPS, highlighting the gaps and areas for future research.

## 2.2. Security Challenges

In the rapidly evolving technological landscape, security challenges remain critical, particularly in smart grids, Battery Management Systems (BMSs), and IoT frameworks. These challenges significantly impact system reliability, integrity, and user privacy.

A study by provides an overview of cyber-physical security issues in BMSs and the adoption of blockchain technology as a cybersecurity measure. The work of emphasizes vulnerabilities in lithium-ion battery systems, such as unauthorized access, DDoS attacks, malware injection, and data manipulation. These threats can affect both the cyber and physical layers of the BMSs with potentially severe consequences, such as compromising battery systems' safety, performance, and lifespan. All these collectively emphasize the necessity of efficient data communication technologies for designing and maintaining the present and emerging smart grids, EVs, and CPSs, along with identifying the future scope. In addition, highlighted these challenges and avenues for research in these nascent technologies to improve the scalability, security, development, and integration capabilities of blockchain-based systems with the performance and resilience afforded by machine learning-based systems [16].

In the context of smart grids, survey the network security challenges addressing threats to data confidentiality, integrity, and availability. And find out that large-scale sensor networks and communication infrastructures are vulnerable. Detection and mitigation techniques to safeguard against cyber threats targeting various network layers, from customer access points to backend management systems, were explored by. These protection measures are offensive security techniques across the network layers, from the consumer access points to backend management systems, as discussed in the survey's results underscored that securing every network infrastructure layer was critical to avoid unauthorized intrusions, data alteration, and service outages. Using strong encryption, multi-factor authentication, and virtual real-time threat detection systems, the study underscored a comprehensive cybersecurity strategy for smart grids, protecting both physical and digital parts from a wide spectrum of emerging threats [23].

The study of IoT resource constraints require lightweight computations, but Distributed Ledger Technology's (DLT) consensus mechanisms are power-intensive. Despite these drawbacks, cryptographic techniques and decentralization strengthen data security, lowering risks like unauthorized access and system failures. The study examines DLT for securing IoT

ecosystems, focusing on distributed data management, immutable records, and enhanced privacy. Identified the main obstacles to integrating DLT with IoT, such as scalability problems, poor throughput, storage limitations, and energy limits. The computational capacity of IoT devices is insufficient for consensus mechanisms, and storage constraints make it challenging to maintain a local ledger copy. Additionally, time-consuming consensus methods raise expenses, restricting scalability. Even while DLT improves security, its current implementation is not feasible for the IoT and needs more investigation and improvement [1].

The work of reviews security challenges in public transport networks, focusing on both current and emerging issues. Current challenges include a need to balance convenience, privacy, interoperability, in addition to addressing skills requirements gap. However, mechanisms to provide data from public transportation systems are still challenged with providing security measures adequate for consumer privacy while securely communicating between different technologies and platforms [39]. Moreover, the greater use of IoT and connected systems in transport infrastructure brings with it added complexity for dealing with these security challenges [39].

For the future, it is very likely that challenges are expected because of increasingly data-driven public transport networks (and greater integration with smart technologies), as already identified. These factors include the protection of user and service provider data in these more data-driven mobility ecosystems, or the consideration of how security solutions are designed and judged as they evolve over time. In addition, this provides vital information for aiding security improvements as an applied technology for public safety and several passenger behavior forecasts under a data protection regulation viewpoint. This work reinforces the need for reliable and adaptable security solutions to ensure that public transport remains trustworthy while not falling behind in technological advancement.

These studies collectively highlight the prevalence of security breaches in IoT systems but often lack practical solutions tailored to the unique demands of EV-IoT integration. Existing security measures are often reactive rather than proactive, and there is a lack of a proactive security framework designed specifically for the EV-IoT ecosystem.

## 2.3. Blockchain Technology

Blockchain is an emerging technology that is decentralized based. It is a transformative paradigm across various sectors that harness attention in academia and industry. Blockchain is a peer-to-peer and transparent network accepted in fields such as Intelligent Transportation Systems (ITS), energy management, and cybersecurity. This decentralized network has many great specifications, such as transparency, immutability, irreversibility, and auditability. Blockchain is proposed as a disruptive and unique technology for realizing distributed ledgers. Despite these [15], identified several challenges faced by blockchain. Particularly unclear regulations and lack of standardization, lack of interoperability between different platforms and partnerships, high energy consumption, especially with the Proof of Work (PoW) consensus protocol, security risks, including smart contract vulnerabilities and 51% majority attacks. Systematically reviews blockchain applications to ITS and the IoV It also points at the potentials of blockchain for the enhancement of data integrity, transparency, and security of transportation logistics, supply chain management, and social IoV environments. Table 1 presents the summary of the reviewed studies.

Table 1. Summary of the related work.

| Ref | Paper type | Type of study | Focus |
|---|---|---|---|
| **[22]** | Survey | Different methodologies for DSM | The paper focuses on applying various methodologies for DSM in modern power grids. |
| **[39]** | Review | EV communication and control domain | importance of efficient communication protocols, standards, and computational technologies for improving the performance, efficiency, and security of Vehicle-to-Grid (V2G), and Grid-to-Vehicle (G2V) communication |
| **[38]** | SLR | Blockchain applications on the IoV | It focuses on the opportunities, taxonomies, and applications of blockchain technology, as well as basic cryptography. |
| **[37]** | Review | Security | The paper focuses on the cyber-physical security of BMSs and the adoption of blockchain technology |
| **[31]** | Review | Power-distribution architectures, protection techniques for smart grids | Focus to enable the research community in the areas of power electronic hardware, control techniques, and communication technology to develop integrated CPS solutions for smart grid. |
| **[18]** | Survey | Cybersecurity challenges on smart grid | Focuses on cybersecurity challenges, detection, and mitigation techniques for the smart grid. |
| **[48]** | Survey | The energy trading mechanisms used in the smart grid | The paper focuses on energy trading in the smart grid, specifically addressing the challenges and solutions associated with designing energy trading mechanisms in this context. |
| **[21]** | Review | Analysis of DLT | Focus the integration of DLT with IoT systems and identifying the challenges associated with this integration |
| **[33]** | Survey | smart meters, smart sensors, vehicle-to-grid technologies | The paper focuses on providing a survey of smart grid technologies and applications. |
| **[24]** | Review | Operational security challenges | This paper focuses on security challenges for public transport networks, emerging future security challenges, and technologies that will impact public transport security in the future. |

Its decentralized and tamper-resistant nature creates trust among all stakeholders while multiple applications give full optimization of ITS operations. Still, there are major limitations in terms of performance, such as restrictions in throughput, latency issues, and bottlenecks within the network, which are further aggravated with the

peer-to-peer architecture of blockchain. This is essentially because the scalability is limited by the very nature of sequential storage of blocks along with complex interlinking, which conventional database systems avoid. Such solution proposals include parallel data structures, enhanced consensus mechanisms, and parallel-chain composition methods. In all these cases, they would do well to remove some of the problems. Security is still one of the leading concerns, considering that blockchain systems can become the targets of DDoS attacks, and shortcomings in the algorithms for cryptographically ensuring operation. Emphasis in future studies shall be on how to strengthen blockchain against different types of vulnerabilities and, in support of high-performance, scalable applications.

Similarly, underscores that blockchain plays the key role in ensuring that the energy storage systems remain tamper-proof as, at every stage, the records concerning battery performance indicators become immutable and thus more reliable and resistant to every kind of cyber-attack. Kim *et al*. [16] highlighted the potentialities of blockchain in mitigating the security vulnerabilities of the BMSs and moving toward resilience and security in the energy infrastructure.

### 2.4. Electronic Vehicle (EV)

Vehicles that run on battery-powered energy are known as EVs. They provide an achievable method to lessen greenhouse gas emissions and the transportation sector's dependence on fossil fuels [39]. Battery Electric Vehicles (BEVs), Plug-in Hybrid Electric Vehicles (PHEVs), and Fuel Cell Electric Vehicles (FCEVs) are three different types of EVs [39]. The potential of EVs to reduce emissions while tackling environmental issues is one of the primary motivations for their development and deployment. EVs have zero tailpipe emissions, which improves air quality and lowers greenhouse gas emissions [38]. The EV industry has grown significantly in the last several years. In many areas, the adoption of EVs has been supported by incentives from the government, assistance, and regulatory measures [17].

#### 2.4.1. Data Transmission and Connectivity in EVs

In EVs, data transfer is how different vehicle parts, sensors, and external systems communicate information to make possible features like battery management, autonomous driving, and Vehicle-to-Vehicle (V2V) communication [37]. EVs with telematics systems may perform Over-The-Air (OTA) software upgrades, remote diagnostics, and real-time monitoring. Connectivity is essential for sending and receiving data to ensure effective operation and maintenance [31].

Effective BMS rely on data transfer to monitor battery health, state of charge, and temperature, ensuring optimal performance and longevity [18]. The exchange of sensitive vehicle and driver data raises concerns about data security and privacy, requiring robust encryption and protection mechanisms [48].

EVs can transfer data and power back to the grid in V2G systems, enabling demand response and enhancing grid stability [21]. OTA software updates are essential for keeping EVs updated with the latest features and security patches, reducing the need for physical service appointments [33]. As EVs become more connected, ensuring robust cybersecurity is critical to protect against potential threats and vulnerabilities in data transfer [24].

#### 2.4.2. Security and Privacy Challenges in EVs

EVs data transfer includes gathering and sending both vehicle and personal information. Securing the confidentiality and integrity of this data is a substantial challenge [29]. For automated and networked EVs, Vehicle-to-everything (V2X) communication, which includes V2V and Vehicle-to-Infrastructure (V2I) communication, is important for securing these communications from hackers is a major concern [26]. EV software systems are vulnerable to viruses and cyberattacks. It is important to safeguard the vehicle software against unauthorized access or malware infections. Also, the infrastructure used for EV charging is exposed to both physical and cyberattacks [13]. It is necessary to guarantee the safety of charging stations and the secure exchange of information between cars and charging stations [28].

## 3. Materials and Method

This section outlines the methodology employed for this study. It includes the eligibility criteria, data collecting process, search method, and sources reviewed.

### 3.1. Search String

The PRISMA framework is a highly utilized methodological approach in systematic reviews and meta-analyses. It was developed to ensure that there was transparency, completeness, and consistency in literature reviews by offering structured processes for identifying, selecting, and evaluating relevant studies. The framework usually covers some stages: eligibility criteria setup, comprehensive literature search, and systematic screening to meet the previously set inclusion and exclusion criteria. The PRISMA flow diagram allows researchers to clearly document this process of selecting studies from identification to eventual inclusion of relevant articles. Adherence to PRISMA guidelines, in this case helps reduce biases and ensure comprehensive evidence coverage, which is of tremendous value in fields of complex and dynamic research, as in the EV-IoT ecosystem.

Applying these criteria to a specified publication or search engine highlighted primary studies. The keywords were chosen to encourage the development of study findings that would aid in addressing the study's issues. The following databases were utilized to find these

articles: IEEE Xplore, Scopus, and Web of science. The query terms were used to retrieve the results from the chosen digital libraries. Only "AND" and "OR" were allowed to be used as Boolean operators.

The query terms were: ("Internet of Things" OR "IoT" OR "connected devices" OR "smart devices" OR "sensor network") AND ("Electrical Vehicle" OR "EV" OR "Electric Vehicle" OR "e-vehicle" OR "e-car" OR "electric car" OR "plug-in vehicle" OR "zero-emission vehicle" OR "battery-powered vehicle" OR "electric automobile") AND ("Security" OR "Privacy" OR "data protection" OR "confidentiality" OR "cybersecurity" OR "information security") ("data transmission" OR "communication" OR "message exchange" OR "information sharing") Shown Figure 1 PRISMA diagram.

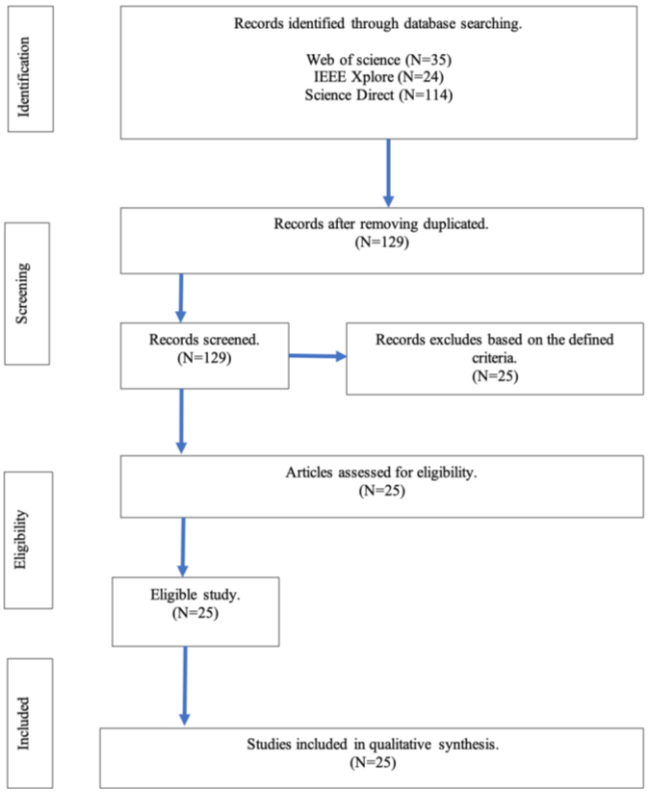


Figure 1. PRISMA.

### 3.2. Motivation

The motivation of improving data transmission in IoT-enabled EVs are data privacy, scalability, and performance. Safety monitoring, battery optimization, and emergency response all depend on performance. Strong privacy regulations safeguard user data and foster confidence, while scalability guarantees seamless operation as EV fleets expand. Secure and effective data transfer will influence the development of intelligent, sustainable transportation in the future as the EV industry grows.

### 3.3. Inclusion Criteria

To ensure relevance, papers were selected based on SLR standards and inclusion-exclusion criteria. Chosen studies focused on:

- IoT integration in EVs.
- Security, privacy, and data protection in IoT-enabled EVs.
- Data transmission and communication in connected EVs.
- Challenges and solutions for EV data security and privacy.
- Technologies and policies for safeguarding EV data exchange.

### 3.4. Exclusion Criteria

The exclusion criteria eliminated studies that lacked IoT-EV convergence, including:

- Research focusing solely on IoT or EVs without integration.
- Studies not addressing security, privacy, data transmission, or communication in IoT-connected EVs.
- Papers unrelated to IoT integration in EVs.
- Research on IoT in non-EV contexts.
- Studies lacking relevant insights on IoT-connected EVs.

### 3.5. Data Extraction

Important concepts are extracted using organized templates from a thorough literature analysis on IoT, EVs, security, and data management. Research on IoT-EV ecosystems, transmission, and security is strengthened by data synthesis, which finds patterns and trends.

## 4. Results

The study findings are compiled in this part, which also illustrates the data kinds and transmission techniques that are crucial for EV interaction in the IoV ecosystem.

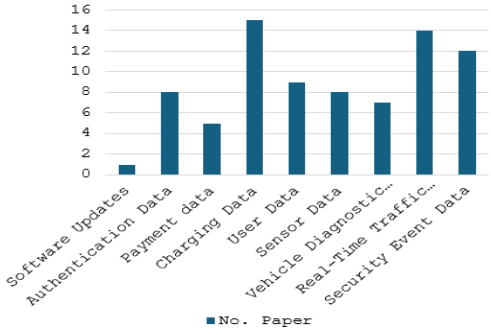


Figure 2. Type of data in EV.

- **Q1: How are Different Types of Data Transmitted between EVs?**

Performance, maintenance, charging, and energy management are all optimized by EV data collecting across many data categories.as shown in Figure 2 above.

Table 2. Type of data in EVs.

| Ref | Software updates | Authentication data | Payment data | Charging data | User data | Sensor data | User data | Vehicle diagnostic data | Real-time traffic data | Security event data |
|---|---|---|---|---|---|---|---|---|---|---|
| [49] | | ✓ | | ✓ | | | | | | ✓ |
| [19] | | | | ✓ | | ✓ | | | ✓ | |
| [42] | | | ✓ | ✓ | ✓ | | ✓ | | | |
| [45] | | | ✓ | ✓ | | | | | | ✓ |
| [5] | | | | ✓ | | ✓ | | | ✓ | |
| [12] | | ✓ | | ✓ | | | | | ✓ | |
| [2] | | ✓ | | | | | | ✓ | | ✓ |
| [6] | | | | | | ✓ | | ✓ | ✓ | |
| [8] | | | | ✓ | ✓ | | ✓ | ✓ | | |
| [25] | | | ✓ | | | | | ✓ | ✓ | |
| [43] | | ✓ | | ✓ | | | | | | ✓ |
| [11] | | | | ✓ | | | | | ✓ | |
| [35] | | ✓ | | | ✓ | | ✓ | | | ✓ |
| [50] | | | | ✓ | | | | ✓ | ✓ | |
| [30] | | ✓ | | ✓ | | | | | | ✓ |
| [20] | | | | | | ✓ | | | ✓ | ✓ |
| [3] | | ✓ | | | | ✓ | | | ✓ | ✓ |
| [41] | ✓ | | | | | | | | | ✓ |
| [47] | | | | ✓ | ✓ | ✓ | ✓ | | | |
| [40] | | | | | ✓ | ✓ | ✓ | | ✓ | |
| [32] | | | | | ✓ | | ✓ | | | ✓ |
| [36] | | | ✓ | ✓ | | | | | ✓ | ✓ |
| [14] | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | |
| [46] | | ✓ | | ✓ | ✓ | | ✓ | | ✓ | |
| [4] | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |

EVs use a variety of sensors and communication techniques to gather and send data. The main data types examined are shown in Table 2. These data types include:

- Software versions: OTA updates are given to EVs to improve their safety and performance. Data integrity and tamper prevention are ensured by secure transmission and user authentication.
- Authentication data: authentication verifies EVs and users, ensuring only authorized access to charging services and trusted networks.
- Payment methods: EV charging involves financial and transactional data exchange, requiring strong encryption to prevent fraud.
- Charging data: charging stations get real-time battery state data for the best scheduling. EV navigation receives station information, including as availability and position.
- User data: financial management, vehicle personalization, and service access are supported by personal information such as name, phone number, and account details.
- Sensor data: EVs can optimize performance, charging, and energy efficiency with the use of environmental data, such as weather, location, and traffic.
- Vehicle diagnostics data: to improve longevity and dependability, EVs produce telematics for diagnostics, transmitting data to manufacturers or service providers for remote analysis and maintenance scheduling.
- Real-time traffic intelligence data: navigation systems save trip time and energy consumption by analyzing traffic to determine the best charging and route options. Unauthorized access is one example of a security event that sets off alarms and procedures to safeguard the IoV ecosystem.
- Data transmission: effective in-vehicle communication is made possible by Controller Area Network (CAN), which EV sensors utilize to track user involvement, battery health, and performance. Wireless transmission of processed data is another option for remote monitoring.

- **Q2: What are the Privacy Risks Associated with the Transmission of EV Data?**

The transmission and dissemination of data from EVs pose numerous privacy hazards and issues that can affect both individual EV owners and the wider society. These hazards include potential security flaws, unlawful privacy intrusions, and the inadvertent disclosure of sensitive personal information. Establishing and implementing robust security and privacy measures is essential for effectively managing and mitigating these risks, as seen in Figure 3.

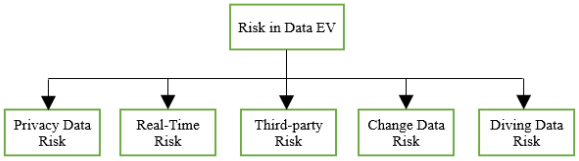


Figure 3. Data risk in EV.

The principal concerns to privacy in this setting

encompass unauthorized access and use of personal data, continuous location surveillance, and the potential for data breaches during transmission. EVs continuously collect real-time location data, which is then disseminated to many external entities, including charging networks and traffic management systems. This data is essential for enhancing service delivery, although it may be obtrusive, raising considerable privacy concerns for end-users [27].

Moreover, the complexities of data-sharing agreements within the EV charging infrastructure intensify the challenges associated with privacy concerns. These agreements may, in specific situations, reduce persons' control over their personal data, therefore prompting inquiries about the informed permission purportedly provided for the acquisition and subsequent use of this information [49].

For example, information exchanged among charging stations, energy suppliers, and third-party platforms may unintentionally be accessed by unauthorized parties, therefore compromising privacy and the integrity of data utilization.

To mitigate these risks, a comprehensive strategy utilizing diverse privacy-preserving technology and legal measures may be implemented. The use of encryption and secure communication protocols is essential for protecting data integrity during transmission, ensuring it is resistant to unwanted access or hostile interference. The deployment of advanced authentication procedures is essential to avert illegal access to EV systems and their data. These techniques must be augmented by secure network connections and routine software updates to successfully close possible security vulnerabilities. The creation of extensive regulatory frameworks can ensure proper governance for data collection and usage, guaranteeing that personal information is managed with the necessary accountability and compliance with data protection laws, such as General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA). These frameworks may also impose more rigorous requirements for acquiring user consent for the processing and distribution of personal data.

Furthermore, the advancement and implementation of sophisticated anonymization methods and data minimization strategies are essential to enhance the protection of sensitive user information. The elimination of identifying characteristics from location data and the limitation of shared personal information might significantly mitigate the privacy threats linked to electric vehicle data transfer.

- **Q3: What are the Existing Techniques for Protecting the Privacy of Transmitted EV Data?**

Data transmission from EVs must ensure privacy because the automotive industry is becoming increasingly data driven. A large amount of data is produced by EVs, including location to battery state, and this data frequently must be shared with a variety of parties, such as manufacturers, service providers, and government agencies. However, it is essential to use a variety of strategies and technologies to guarantee the security and confidentiality of sensitive data. These techniques will provide a set on the wide range of methods at the center of protecting EV data in transit shown in Table 3 and Figure 4, whether these methods be encryption, anonymization, access control, or upcoming technologies like differential privacy and blockchain.

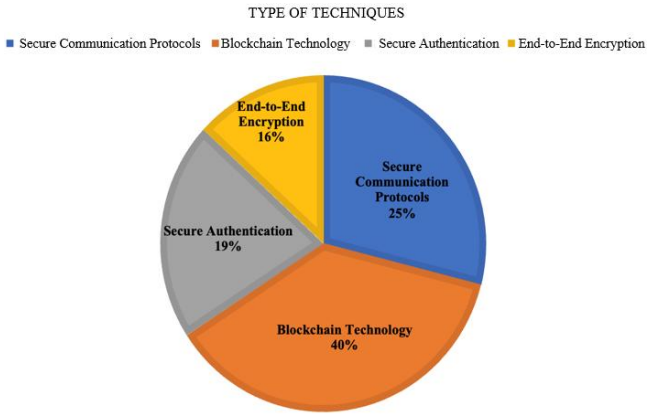


Figure 4. Type of techniques used to protect data in EV.

Table 3. Techniques or methods used in protection data transmission.

| Ref. | Secure communication protocols | Blockchain technology | Secure authentication | End-to-end encryption |
|---|---|---|---|---|
| [49] | | ✓ | | |
| [19] | ✓ | | | |
| [42] | ✓ | | | |
| [45] | | ✓ | | |
| [5] | | | ✓ | ✓ |
| [12] | | ✓ | | |
| [2] | ✓ | | | |
| [6] | | ✓ | | |
| [8] | | | | ✓ |
| [25] | ✓ | | | |
| [43] | ✓ | | ✓ | |
| [11] | ✓ | | ✓ | |
| [35] | ✓ | | | |
| [50] | | ✓ | | |
| [30] | | | | ✓ |
| [20] | | | ✓ | |
| [3] | | ✓ | | |
| [41] | | ✓ | | |
| [47] | | ✓ | | ✓ |
| [40] | | ✓ | | |
| [32] | ✓ | | ✓ | |
| [36] | | ✓ | | |
| [14] | | ✓ | | |
| [46] | | ✓ | | |
| [4] | | ✓ | ✓ | |
| [9] | | ✓ | ✓ | |

- **Q4: What Challenges Are Encountered in the Processes of Storing, Gathering, and Transmitting Data within EVs?**

EVs present challenges in terms of data storage, collection, and transmission due to the complexity of the data, the need for real-time processing, and the

requirement for system reliability and security. Designed a secure key exchange scheme for the secure transmission of data in a smart grid environment. Cloud and fog/edge computing models enable the acquisition of charging profiles of EVs and the transmission of data to a central database in the cloud [42].

1. Data storage in EVs:
   a) Limited storage capacity.
   b) Policy for data storage.
2. Data Security Gathering data in EVs.
3. Data Calibration and Accuracy
4. Transmitting data in EVs:
   a) Bandwidth limitation.
   b) Security of networks.
   c) Connection problems.

## 5. Discussion

This section evaluates key findings and identify knowledge gaps based on emerging themes. Also, it presents a critical analysis drawn from the literature reviewed. The section is further categorized into five sub-sections for better organization and discussion.

### 5.1. Findings in Data Types Used in EVs

In this section, we are studying the types of data in EV, as well as the methods of sending them, we explored that were not addressed or mentioned in published studies, such as system updates data in EV. We note the focus of these studies on charging data as well as on real-time data. Through the evaluation of all these studies, we note that no study has studied all the data in EV while studying one type of data or several types of data in EV.

### 5.2. Limitation for Each Technique Used

The difficulties with different security methods in the IoV ecosystem are addressed in this section. Although data encryption secures protected communication, it increases computing overhead, which makes it less practical for EVs with limited resources. Although blockchain improves security, it has problems with scalability and energy efficiency. In the event of a network outage or authentication failure, OTA updates run the danger of being exploited. Although biometric authentication increases security, device heterogeneity and privacy issues make deployment more difficult.

We hope to explain the complex relationship between the models used in IoV research and where further work is needed. Areas for future research include developing models that combine safety and efficiency, ensuring that scaling does not mean sacrificing data quality, or techniques that address privacy while preserving the real-time behavior so desirable for EV performance. In identifying these gaps, we encourage other researchers to build on what they already have, intending to provide comprehensive, scalable, and secure solutions for an IoV transition targeting the following limitations:

- Secure communication protocols: these include
- Requirements for standardization and connectivity, the risk of OTA updates, resource limitations in EV systems, complexity and compatibility challenges, privacy concerns about protecting sensitive data, and vulnerability to cyberattacks.
- Blockchain technology: latency is the main obstacle to using blockchain technology for EV applications. Most blockchain consensus algorithms include a natural latency in transaction processing, which could delay real-time data transmission essential to EV operations. High latency can interfere with vehicle-to-vehicle communication, grid interactions, and charging transactions, making it difficult for the EV ecosystem to function efficiently and rapidly.
- Secure authentication: these include possible cyberattacked-exploitable limitations in authentication protocols, the possibility of illegal access to vehicle systems, difficulties striking a balance between security and user experience, and the requirement for strong defenses against changing cybersecurity threats. These methods focused primarily on protecting against unauthorized access and ensuring user privacy and safety.
- End-to-end encryption: these include the requirement for standardized and compatible encryption standards across different EV platforms, the possibility of increased computational costs affecting real-time communication, and potential difficulties in implementing and managing complex encryption processes within resource-constrained EV systems. These restrictions are essential for protecting sensitive data transmitted inside EVs from potential security risks and maintaining such data's confidentiality and integrity.

### 5.3. Model and Gaps for Each Study Used

In this section, we will explore the models used in each research, identifying the weaknesses in their frameworks. Our goal is to mention a comprehensive gap in the approaches shown in Table 4 and identify the disadvantages of the selected models. Our goal is to present a thorough summary that explains the complex interaction between the models used and the possible areas in which more investigation or improvement may be necessary. Moreover, gaps for the related studies in EV are but not limited to the following points presented in Table 4.

Table 4. Challenges and limitations in recent security and privacy solutions.

| Ref. | Model | Scalability | Computational complexity and efficiency | Security and privacy concerns | Real-time responsiveness | Data integrity and security | Integration complexity |
|---|---|---|---|---|---|---|---|
| **[49]** | Chebyshev chaotic map | Not addressed | Not addressed | Not addressed | Not addressed | not addressed | limited theoretical analysis, and the need for standardized implementations |
| **[42]** | Data driven V2V matching protocol | Not addressed | Not addressed | Not addressed | Not addressed | Used single point to save information, used two stages offline and online these cause delay | Not addressed |
| **[45]** | Blockchain-based secure incentive scheme and PoR consensus | Scalability issues as the computational demands for research verification increase with the growing network size | Not addressed | Not addressed | Not addressed | Not addressed | Not addressed |
| **[5]** | Holistic framework and distributed consensus innovations | Not addressed | The holistic framework could lead to increased computational overhead and resource demands and complexity | Not addressed | Not addressed | Not addressed | Not addressed |
| **[2]** | Lightweight key agreement protocol using lightweight cryptographic operations such as exclusive-OR and hash | Not addressed | Not addressed | Effect on security, and scalability concerns for broader application | Not addressed | Not addressed | Not addressed |
| **[6]** | Intrusion Detection System (IDS) | The interpretability and explain ability of alerts, the scalability of IDS to handle large and complex networks | Not addressed | Not addressed | Not addressed | Not addressed | Not addressed |
| **[8]** | Multi-layer Cyber-Physical-Social Systems (CPSS) | Not addressed | Not addressed | Not addressed | Not addressed | Not addressed | Managing complexity across interconnected layers effectively. Issues related to information flow and trust across layers. |
| **[43]** | End-to-end secured | Not addressed | Not addressed | Not addressed | Increased computational overhead affecting real-time communication | Not addressed | Not addressed |
| **[11]** | Cyber physical operator (CPO) | Not addressed | Not addressed | Not addressed | Real-time responsiveness and reliability of CPO systems, complexities in integrating CPO with diverse EV platforms | Not addressed | Not addressed |
| **[30]** | Authentication protocols for CWD-WPT charging systems | Not addressed | Not addressed | Complexities in managing secure communication protocols | Not addressed | Not addressed | Not addressed |
| **[3]** | Elliptic curve cryptosystem-based hybrid signcryption | Not addressed | Not addressed | Key management complexity, computational overhead, standardization and interoperability | Not addressed | Not addressed | Not addressed |
| **[41]** | Approximate algorithm | Not addressed | Sensitivity to data quality, limited adaptability to real-time changes | Not addressed | Not addressed | Not addressed | Not addressed |
| **[46]** | Blockchain, zero-knowledge proof and ring-signature | Not addressed | Zero-Knowledge Proof (ZKP) and ring signatures can be computationally expensive, especially for large messages or complex computations. | Not addressed | Not addressed | Not addressed | Not addressed |

## 5.4. Evaluating the Studies

This section provides a systematic evaluation of selected test results, concentrating on four aspects that are central to the assessment: performance, scalability, storage, and privacy/security, as detailed in Figure 5 and Table 5. Through these comparisons, this study offers a rounded picture of how strong or weak each specimen is to help better understand its efficacy and robustness.

- Performance: real-time data transmission and processing speed were evaluated in the studies. Real-time responses in dynamic charging scenarios are made possible by models that use OCPP and ISO 15118. However, EV-to-grid connections that employ high-computation security mechanisms, like as blockchain, may have considerable latency.
- Scalability: many models struggle with enormous networks however perform well in experiments conducted on a small scale. Growing EV needs cause centralized systems to fail, while blockchain has scalability problems such as slow transactions and excessive energy consumption. 5G delivers low-latency, high-volume transmission but confronts implementation issues.
- Storage: data storage is still a major problem. High capacity is provided by cloud storage, but there is a chance of malfunctions and security problems. Although it is expensive and has a limited capacity, blockchain guarantees security. By processing data locally, edge computing increases efficiency, but it might affect real-time performance.
- Privacy and security: in the transmission of IoV data, security and privacy are crucial. Although encryption ensures security, it affects speed. Because blockchain is transparent, it compromises privacy even while it prohibits manipulation. Although they are still in the experimental stage, advanced techniques like ZKP and homomorphic encryption promise.

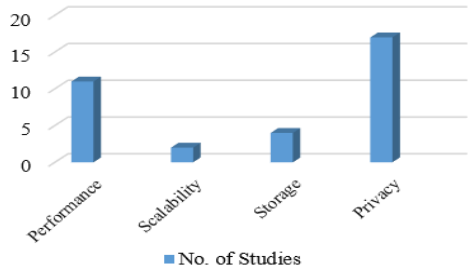


Figure 5. Evaluation results of each study.

This extensive review aims to give readers an integrated evaluation of all studies' strengths and limitations in each area. By understanding each model's real-time capability, storage efficiency, scalability, and privacy/security, we aim to provide a nuanced overview that considers the multifaceted nature of the papers evaluated. This assessment draws attention to researchers' trade-offs when developing robust, scalable solutions for a changing IoV environment.

Table 5. Evaluate each study.

| Ref. | Performance | Scalability | Storage | Privacy |
|---|---|---|---|---|
| [35] | ✓ | | | ✓ |
| [19] | | | | ✓ |
| [42] | | | | ✓ |
| [45] | ✓ | ✓ | | |
| [5] | | | | ✓ |
| [12] | | | | ✓ |
| [2] | | | | ✓ |
| [6]] | | | | ✓ |
| [25] | | | | ✓ |
| [43] | | | | ✓ |
| [43] | | | | ✓ |
| [11] | ✓ | | | |
| [35] | ✓ | | | |
| [50] | ✓ | | | ✓ |
| [30] | ✓ | | | ✓ |
| [20] | | | ✓ | ✓ |
| [3] | | | ✓ | |
| [41] | | | ✓ | |
| [47] | | | | ✓ |
| [40] | ✓ | | | ✓ |
| [32] | ✓ | | | ✓ |
| [36] | ✓ | ✓ | | |
| [14] | ✓ | | | ✓ |
| [46] | ✓ | | | |
| [4] | | | ✓ | |
| [9] | ✓ | | | ✓ |

## 5.5. Proposed Model

We propose a Hybrid Blockchain-Based (HBB) model to address the identified challenges in data transmission, security, and scalability of the IoV ecosystem. It combines the strengths of blockchain technology with edge computing to ensure secure, efficient, and scalable data transmission. Previous research into EV charging networks using blockchain technology has significantly improved security and data integrity. Thus, this study takes this work further with a hybrid blockchain architecture for even greater scalability and real-time data transmission, as shown in Figure 6. This model consists of three basic layers: the EV layer, the Edge Computing layer, and the blockchain layer. The EV layer engages immediately with the edge node for efficient and focused on choices. The edge computing layer manages high-frequency data in real-time, filtering unnecessary data to reduce latency and bandwidth consumption. The blockchain layer guarantees immutability and decentralized validation of important information using a permissioned blockchain model for enhanced throughput.

The proposed HBB Framework for secure and scalable data transmission in IoV integration, which is a combination of edge computing with blockchain enables privacy-preserving data transmission to support security functions such as confidentiality, integrity and scalability. This design allows decentralized authentication processes, thus eliminating the requirement for centralized trust models. It also improves latency-sensitive processes, such as charging session start, routing, and identifying defects, by facilitating real-time edge processing.

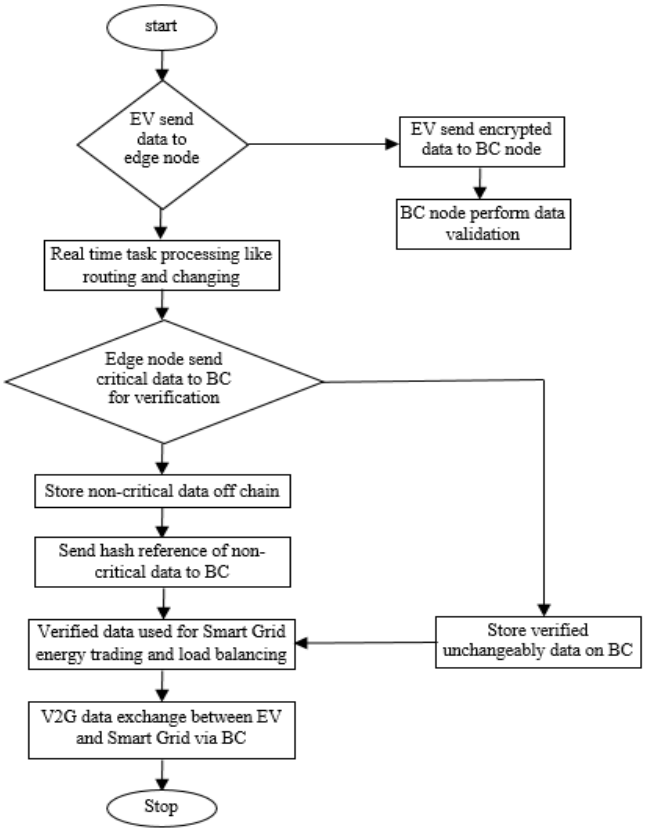


Figure 6. Proposed model.

This model eliminates the need for EVs to send critical data (e.g., battery status, location etc.) all the way to cloud instances and enables real-time processing at nearby edge nodes (e.g., charging reservations) using blockchain frameworks where only essential transactions are efficiently validated and stored on a blockchain network employing lightweight consensus algorithms such as PoS By reducing dependence on cloud storage and using PoS, the system significantly decreases energy usage and enhances transaction speed, rendering it more appropriate for IoV settings where response is important. Off-chain storage is storing non-critical data that helps to keep the blockchain light. This include telemetry data, diagnostic logs, or historical use data, which may be related on-chain using cryptographic hash pointers to preserve integrity without expanding the blockchain ledger. Homomorphic encryption and zero-knowledge proofs also enable the secure exchange of data, which prevents sensitive data from being leaked. Homomorphic encryption facilitates computations on encrypted data without requiring decryption, while zero-knowledge proofs enable the verification of data accuracy without providing the real data. These solutions enhance privacy protections and facilitate compliance to rules (e.g., GDPR) for global IoV implementations.

Further, the framework is also interoperable with smart grid-based energy management and receiving/sending V2G communication for optimal data sharing between any entities in the IoV ecosystem. The blockchain layer enables automated vehicle-to-grid energy trading using smart contracts, enabling EV to function as mobile energy storage units. This unidirectional connection improves load balancing and dynamic pricing systems between the grid and EV, therefore advancing the concept of a decentralized, intelligent transportation and energy network.

## 5.6. Practical Implications of the Proposed Model

- The principal components of the V2G system include:
  1. EV: act as both energy consumers and suppliers, sharing battery and user data.
  2. Smart charging station: Interface between EVs and the grid, managing energy flow.
  3. Smart grid: adjusts demand, facilitates energy trade, and ensures secure data exchange.
  4. Edge nodes: process real-time data on energy capacity and pricing locally.
- Using the proposed model, the implementation steps are:
  5. To protect privacy and facilitate secure data exchange, EVs use homomorphic encryption to gather and encrypt information about charging, energy availability, location, and preferences.
  6. Edge node processing: for processing in real time, EVs transmit encrypted data to adjacent edge nodes, such as charging stations. By sending only necessary information across the blockchain, including energy availability and prices, edge nodes lower latency.

7. Blockchain for energy trading: the availability, cost, and grid usage of EV energy is recorded in a blockchain transaction. Secure, inexpensive verification by energy suppliers or charging stations is ensured by lightweight consensus methods. After verification, the deal is carried out by the V2G system, which updates the grid and permanently records all information for complete transparency.
8. Store non-essential data on off-chain storage: the blockchain's integrity is maintained using hashes, while non-essential data, like as user preferences and transaction history, is kept off-chain. By reducing network request, this enhances scalability as EV use increases.
9. Privacy and security guarantee: zero-knowledge proofs verify energy availability without providing specifics about the battery. Homomorphic encryption ensures anonymity in V2G transactions by processing data without leaking its content.

### 5.7. Recommendation

Implementing modern protocols like OCPP and IEEE 2030.5 is crucial for secure payment and grid management to enhance data transfer and security in IoV ecosystems. To manage EV-generated data and provide scalability and real-time processing, a robust big data infrastructure is required. Blockchain improves security by avoiding data modification and unauthorized access, but its scalability and energy consumption need hybrid security models and efficient consensus processes. Universal protocols can reduce inefficiencies and data loss by achieving interoperability across systems. The recommendations, which are based on the CPS framework, improve security, control, and real-time monitoring while promoting sustainable smart grids. This study examined blockchain applications, security issues, and IoV data transmission; however, it discovered limitations in data spectrum coverage, scalability, and real-time response. To ensure secure and efficient data transfer for sustainable transportation, future studies should concentrate on platform interoperability, integrated data protocols, and efficient blockchain solutions.

## 6. Future Trends

A major solution for IoT-EV integration is lightweight blockchain technology, which provides improved security, efficiency, and transparency with less processing overhead. It improves invoicing and infrastructure management by facilitating secure data exchange between automakers, service providers, and government agencies. Through decentralized peer-to-peer energy trading, blockchain integration with IoT improves EV energy management while lowering grid load and increasing the usage of renewable energy sources. Additionally, it improves traffic flow and urban mobility by enhancing V2X connection, which enables EVs to communicate with smart city infrastructure. Blockchain technology protects EV systems against hackers by ensuring secure software upgrades. Furthermore, its cryptographic features protect private user information, protecting connected vehicles' privacy and trust. With all factors considered, lightweight blockchain is a novel technology that is affecting the development of EV and making the EV ecosystem more connected, secure, and effective.

## 7. Conclusions

This research surveyed blockchain's purpose in the IoV ecosystem, security issues, and data transfer. Current models find it difficult to satisfy the desire for secure, real-time data processing, which has been illustrated by the rapid development of the Internet of Things and EVs. Scalability and efficiency depend on strong big data infrastructure and complex protocols like OCPP and IEEE2030.5. Blockchain provides robust protection against online attacks, but it has drawbacks like high energy costs and constrained scalability. To improve efficiency, future research should concentrate on merging hybrid models and refining consensus methods like PoS. Standardized protocols may be used to ensure interoperability throughout the IoV ecosystem, ensuring secure and simple data sharing. The security and resilience of the smart grid may be improved by integrating blockchain technology with commonly used protocols. This integration, which is compatible with the CPS architecture, improves cybersecurity and real-time monitoring, ensuring a secure and efficient IoV environment. Policymakers to use the recommended solutions. Through improved stakeholder engagement, industrial interests and the public interest must be balanced to integrate IoV into a smart grid that is secure, efficient, and sustainable. Blockchain is just one of several modern technologies required to improve the security and scalability of smart grids, but it provides possible answers. Continuous research and policy adaption are crucial to maintaining a resilient infrastructure as technology advances. Only by addressing the issues identified in this study can the environmental, financial, and technological advantages that the advent of EVs provides be completely achieved. Globally, a stable and sustained IoV ecosystem is made possible by resolving these problems.

## Acknowledgments

This work was supported by the Dato' Low Tuck Kwong International Energy Transition Grant under the project code of 202202002ETG.

## References

[1] Aggarwal S., Kumar N., Tanwar S., and Alazab M., "A Survey on Energy Trading in the Smart Grid:

Taxonomy, Research Challenges and Solutions," *IEEE Access*, vol. 9, pp. 116231-116253, 2021. DOI:10.1109/access.2021.3104354

[2] Ahmed S., Kumari S., Saleem M., Agarwal K., Mahmood K., and Yang M., "Anonymous Key-Agreement Protocol for V2G Environment within Social Internet of Vehicles," *IEEE Access*, vol. 8, pp. 119829-119839, 2020. DOI:10.1109/ACCESS.2020.3003298

[3] Ali I., Chen Y., Pan C., and Zhou A., "ECCHSC: Computationally and Bandwidth Efficient ECC-Based Hybrid Signcryption Protocol for Secure Heterogeneous Vehicle-to-Infrastructure Communications," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4435-4450, 2022. DOI:10.1109/JIOT.2021.3104010

[4] Alshaeri A. and Younis M., "A Blockchain-Based Energy Trading Scheme for Dynamic Charging of Electric Vehicles," *in Proceedings of the IEEE Conference on Global Communications*, Madrid, pp. 1-6, 2021. DOI:10.1109/GLOBECOM46510.2021.9685296

[5] Amini M., Mohammadi J., and Kar S., "Distributed Holistic Framework for Smart City Infrastructures: Tale of Interdependent Electrified Transportation Network and Power Grid," *IEEE Access*, vol. 7, pp. 157535-157554, 2019. DOI:10.1109/ACCESS.2019.2950372

[6] Basavaraj D. and Tayeb S., "Towards a Lightweight Intrusion Detection Framework for in-Vehicle Networks," *Journal of Sensor and Actuator Networks*, vol. 11, no. 1, pp. 1-20, 2022. DOI:10.3390/jsan11010006

[7] Beecroft M., "The Future Security of Travel by Public Transport: A Review of Evidence," *Research in Transportation Business and Management*, vol. 32, pp. 100388, 2019. DOI: 10.1016/j.rtbm.2019.100388

[8] Cali U., Kuzlu M., Elma O., Gucluturk O., Kilic A., and Catak F., "Cybersecurity and Digital Privacy Aspects of V2X in the EV Charging Structure," *in Proceedings of the European Interdisciplinary Cybersecurity Conference*, Stavanger, pp. 174-180, 2023. DOI:10.1145/3590777.3591406

[9] Dhulavvagol P., Totad S., and Anagal A., "SHARD-FEMF: Adaptive Forensic Evidence Management Framework Using Blockchain Sharding and IPFS," *The International Arab Journal of Information Technology*, vol. 21, no. 2, pp. 179-190, 2024. DOI:10.34028/iajit/21/2/1

[10] Dileep G., "A Survey on Smart Grid Technologies and Applications," *Renewable Energy*, vol. 146, pp. 2589-2625, 2020. DOI: 10.1016/j.renene.2019.08.092

[11] Dong C., Li X., Jiang W., Mu Y., Zhao J., and Jia H., "Cyber-Physical Modelling Operator and Multimodal Vibration in the Integrated Local Vehicle-Grid Electrical System," *Applied Energy*, vol. 286, pp. 116432, 2021. DOI: 10.1016/j.apenergy.2021.116432

[12] Erdin E., Cebe M., Akkaya K., Solak S., Bulut E., and Uluagac S., "Building a Private Bitcoin-Based Payment Network among Electric Vehicles and Charging Stations," *in Proceedings of the IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data Conferences*, Halifax, pp. 1609-1615, 2018. DOI:10.1109/Cybermatics_2018.2018.00269

[13] Gazdar T., Alboqomi O., and Munshi A., "A Decentralized Blockchain-Based Trust Management Framework for Vehicular Ad Hoc Networks," *Smart Cities*, vol. 5, no. 1, pp. 348-363, 2022. DOI:10.3390/SMARTCITIES5010020

[14] Hassija V., Chamola V., Garg S., Krishna D., Kaddoum G., and Jayakody D., "A Blockchain-Based Framework for Lightweight Data Sharing and Energy Trading in V2G Network," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5799-5812, 2020. DOI:10.1109/TVT.2020.2967052

[15] Jabbar R., Dhib E., Said A., Krichen M., Fetais N., and Zaidan E., "Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review," *IEEE Access*, vol. 10, pp. 20995-21031, 2022. DOI:10.1109/ACCESS.2022.3149958

[16] Kim T., Ochoa J., Faika T., Mantooth H., Di J., and Li Q., "An Overview of Cyber-Physical Security of Battery Management Systems and Adoption of Blockchain Technology," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 1, pp. 1270-1281, 2022. DOI:10.1109/JESTPE.2020.2968490

[17] Li L., Wang Z., and Xie X., "From Government to Market? A Discrete Choice Analysis of Policy Instruments for Electric Vehicle Adoption," *Transportation Research Part A: Policy and Practice*, vol. 160, pp. 143-159, 2022. DOI: 10.1016/J.TRA.2022.04.004

[18] Li S., He H., Wei Z., and Zhao P., "Edge Computing for Vehicle Battery Management: Cloud-based Online State Estimation," *Journal of Energy Storage*, vol. 55, pp. 105502, 2022. DOI: 10.1016/J.EST.2022.105502

[19] Lin Y., Chen Y., Zheng J., Chu D., Shao D., and Yang H., "Blockchain Power Trading and Energy Management Platform," *IEEE Access*, vol. 10, pp. 75932-75948, 2022. DOI:10.1109/ACCESS.2022.3189472

[20] Lu L., Liu J., Zou D., Zhang S., Chen Y., and Zhu K., "Safety Risk Analysis and Safety Protection Measures of Power Distribution Internet of Things," *in Proceeding of the China International Conference on Electricity Distribution*, Shanghai,

pp. 633-637, 2021. DOI:10.1109/CICED50259.2021.9556815

[21] Mahammad M. and Bethi C., "A Review on Electric Vehicle Battery Charging Infrastructure," *in Proceedings of the International Conference on Edge Computing and Applications*, Tamilnadu, pp. 740-744, 2022. DOI:10.1109/ICECAA55415.2022.9936062

[22] Mastoi M., Zhuang S., Munir H., and Haris M., and et al., "An In-Depth Analysis of Electric Vehicle Charging Station Infrastructure, Policy Implications, and Future Trends," *Energy Reports*, vol. 8, pp. 11504-11529, 2022. DOI: 10.1016/J.EGYR.2022.09.011

[23] Mazumder S., Kulkarni A., Sahoo S., Blaabjerg F., Mantooth H., and Balda J., "A Review of Current Research Trends in Power-Electronic Innovations in Cyber-Physical Systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5146-5163, 2021. DOI:10.1109/JESTPE.2021.3051876

[24] Metere R., Pourmirza Z., Walker S., and Neaimeh M., "An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure," *arXiv Preprint*, vol. arXiv:2209.07842v1, pp. 1-12, 2022. https://arxiv.org/abs/2209.07842v1

[25] Moradi J., Shahinzadeh H., Nafisi H., Gharehpetian G., and Shaneh M., "Blockchain, a Sustainable Solution for Cybersecurity Using Cryptocurrency for Financial Transactions in Smart Grids," *in Proceedings of the 24th Electrical Power Distribution Conference*, Khoramabad, pp. 47-53, 2019. DOI:10.1109/EPDC.2019.8903713

[26] Naeem A., Soomro A., Saim H., and Malik H., "Smart Road Management System for Prioritized Autonomous Vehicles Under Vehicle-to-Everything (V2X) Communication," *Multimedia Tools and Applications*, vol. 83, pp. 41637-41654, 2023. DOI:10.1007/S11042-023-16950-1

[27] Panda S., Mohanta B., Dey M., Satapathy U., and Jena D., "Distributed Ledger Technology for Securing IoT," *in Proceedings of the 11th International Conference on Computing, Communication and Networking Technologies*, Kharagpur, pp. 1-6, 2020. DOI:10.1109/ICCCNT49239.2020.9225333

[28] Park K., Park Y., Das A., Yu S., Lee J., and Park Y., "A Dynamic Privacy-Preserving Key Management Protocol for V2G in Social Internet of Things," *IEEE Access*, vol. 7, pp. 76812-76832, 2019. DOI:10.1109/ACCESS.2019.2921399

[29] Rao P., Jangirala S., Pedada S., Das A., and Park Y., "Blockchain Integration for IoT-Enabled V2X Communications: A Comprehensive Survey, Security Issues and Challenges," *IEEE Access*, vol. 11, pp. 54476-54494, 2023. DOI: 10.1109/ACCESS.2023.3281844

[30] Roman L. and Gondim P., "Authentication Protocol in CTNs for a CWD-WPT Charging System in a Cloud Environment," *Ad Hoc Networks*, vol. 97, pp. 102004, 2020. DOI: 10.1016/j.adhoc.2019.102004

[31] Saad M., Khan M., and Ahmad M., "Blockchain-Enabled Vehicular Ad Hoc Networks: A Systematic Literature Review," *Sustainability*, vol. 14, no. 7, pp. 1-31, 2022. DOI:10.3390/SU14073919

[32] Saha R., Kumar G., Geetha G., Kim T., Alazab M., and Thomas R., "The Blockchain Solution for the Security of Internet of Energy and Electric Vehicle Interface," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 7495-7508, 2021. DOI:10.1109/TVT.2021.3094907

[33] Sahin A. and Yang R., "A Survey on Over-the-Air Computation," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 3, pp. 1877-1908, 2023. DOI:10.1109/COMST.2023.3264649

[34] Said D., "A Survey on Information Communication Technologies in Modern Demand-Side Management for Smart Grids: Challenges, Solutions, and Opportunities," *IEEE Engineering Management Review*, vol. 51, no. 1, pp. 76-107, 2023. DOI:10.1109/EMR.2022.3186154

[35] Salas M., Shao S., Salustri A., Schroeck Z., and Zheng J., "Securing Smart Grid Enabled Home Area Networks with Retro-Reflective Visible Light Communication," *Sensors*, vol. 23, no. 3, pp. 1-12, 2023. DOI:10.3390/s23031245

[36] Samuel O., Javaid N., Shehzad F., Iftikhar M., Iftikhar M., Farooq H., and Ramzan M., *Advances on Broad-Band Wireless Computing, Communication and Applications*, Springer, 2020. https://doi.org/10.1007/978-3-030-33506-9_7

[37] Sanguesa J., Torres-Sanz V., Garrido P., Martinez F., and Marquez-Barja J., "A Review on Electric Vehicles: Technologies and Challenges," *Smart Cities*, vol. 4, no. 1, pp. 372-404, 2021. DOI:10.3390/SMARTCITIES4010022

[38] Siraj F. and Mehra P., *Sustainable Growth and Global Social Development in Competitive Economies*, IGI Global Scientific Publishing, 2023. DOI:10.4018/978-1-6684-8810-2.ch013

[39] Souza L., Lora E., Palacio J., Rocha M., Reno M., and Venturini O., "Comparative Environmental Life Cycle Assessment of Conventional Vehicles with Different Fuel Options, Plug-in Hybrid and Electric Vehicles for a Sustainable Transportation System in Brazil," *Journal of Cleaner Production*, vol. 203, pp. 444-468, 2018. DOI: 10.1016/J.JCLEPRO.2018.08.236

[40] Su Z., Wang Y., Xu Q., Fei M., Tian Y., and Zhang N., "A Secure Charging Scheme for Electric Vehicles with Smart Communities in Energy Blockchain," *IEEE Internet of Things Journal*, vol.

6, no. 3, pp. 4601-4613, 2019. DOI:10.1109/JIOT.2018.2869297

[41] Tang X., Bi S., and Zhang Y., "Distributed Routing and Charging Scheduling Optimization for Internet of Electric Vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 136-148, 2019. DOI:10.1109/JIOT.2018.2876004

[42] Tao Y., Qiu J., Lai S., Sun X., Wang Y., and Zhao J., "Data-Driven Matching Protocol for Vehicle-to-Vehicle Energy Management Considering Privacy Preservation," *IEEE Transactions on Transportation Electrification*, vol. 9, no. 1, pp. 968-980, 2023. DOI:10.1109/TTE.2022.3188766

[43] Terruggia R. and Garrone F., "Secure IoT and Cloud Based Infrastructure for the Monitoring of Power Consumption and Asset Control," *in Proceeding of the AEIT International Annual Conference*, Catania, pp. 1-6, 2020. DOI: 10.23919/AEIT50178.2020.9241195

[44] Tufail S., Parvez I., Batool S., and Sarwat A., "A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid," *Energies*, vol. 14, no. 18, pp. 1-22, 2021. DOI:10.3390/en14185894

[45] Wang Y., Su Z., and Zhang N., "BSIS: Blockchain-Based Secure Incentive Scheme for Energy Delivery in Vehicular Energy Network," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3620-3631, 2019. DOI:10.1109/TII.2019.2908497

[46] Xu S., Chen X., and He Y., "EVchain: An Anonymous Blockchain-Based System for Charging-Connected Electric Vehicles," *Tsinghua Science and Technology Journal*, vol. 26, no. 6, pp. 845-856, 2021. DOI:10.26599/TST.2020.9010043

[47] Xu Y., He H., Liu J., Shen Y., Taleb T., and Shiratori N., "IDADET: Iterative Double-Sided Auction-Based Data-Energy Transaction Ecosystem in Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 10113-10130, 2023. DOI:10.1109/JIOT.2023.3236968

[48] Yu Z., Gao H., Cong X., Wu N., and Song H., "A Survey on Cyber-Physical Systems Security," *IEEE Internet Things Journal*, vol. 10, no. 24, pp. 21670-21686, 2023. DOI:10.1109/JIOT.2023.3289625

[49] Zhang L., Zhu Y., Ren W., Wang Y., Choo K., and Xiong N., "An Energy-Efficient Authentication Scheme Based on Chebyshev Chaotic Map for Smart Grid Environments," *IEEE Internet of Things Journal*, vol. 8, no. 23, pp. 17120-17130, 2021. DOI:10.1109/JIOT.2021.3078175

[50] Zhang Y., Shang J., Chen X., and Liang K., "A Self-Learning Detection Method of Sybil Attack Based on LSTM for Electric Vehicles," *Energies*, vol. 13, no. 6, pp. 1-15, 2020. DOI:10.3390/en13061382

**Faisal Faisal** received the Bachelor's degree in Software Engineering from Al-Mansour University College, Baghdad, Iraq, in 2009. He then obtained a Master's degree in computer Science from the Department of Computer Science, University of Technology, Baghdad, Iraq, in 2016. Currently, he is working toward the doctoral degree with the Department of Computing (CCI) at UNITEN, Malaysia. His research interests include: The Internet of Things (IoT), Electric Vehicles (EV), and Block-Chain (BC).

**Moamin Mahmoud** obtained his bachelor in Mathematics from the College of Mathematics and Computer Science, University of Mosul, Iraq in 200 7. He obtained his Master of Information Technology at the College of Graduate Studies, University Tenaga Nasional (UNITEN), Malaysia in 2010, and Ph.D. of Information and Communication Technology from University Tenaga Nasional (UNITEN), Malaysia in 2013, he joined University Tenaga Nasional as a Senior Lecturer in the Deptartment of Software Engineering since 2014. He also was awarded a Machine Learning Certification from Cornell University, USA, and a Professional Technologist Certification from the Malaysia Board of Technologists (MBOT), Malaysia. He is currently a deputy Dean (Research and Innovation), College of Computing and Informatics, University Tenaga Nasional. His core Expertise is in Data Analytics and his research interest includes: the Application of Artificial Intelligence Technics to other domains such as health, energy, social, transportation, and drones. Moamin has a thorough knowledge in research and supervision. He has produced more than 100 articles of WoS/Scopus-indexed journals. Under his supervision has successfully graduated more than 50 undergraduates, nine Masters, and five Ph.D. Apart from this, He has secured as leader nine research grants funded from different national and international sources, and 3 consultancy projects with industry. Besides, He also has filed four copyrights and one patent titled "A Computer-Implemented Method and System for Modeling and Predicting Failure of a Power Grid Configuration". He has been invited to assess Master and Ph.D. Thesis and evaluate grant proposals. Last but not least, he served on the Editorial Board/Technical Committee/Reviewer for many journals and conferences.

**Abba Hassan** received his Bachelor's degree in Software Engineering from Infrastructure University Kuala Lumpur, Malaysia, in 2014, followed by a Master's degree in IT, specializing in Software Engineering, in 2015. Currently, he is pursuing a PhD at University Tenaga Nasional, Malaysia. His research interests include: Electric Vehicles, Software Engineering, and Information Systems.

**Salama Mostafa** received a B.Sc. degree in Computer Science from the University of Mosul, Iraq, in 2003 and an M.Sc. and Ph.D. in Information and Communication Technology (ICT) from university Tenaga Nasional (UNITEN), Malaysia, in 2011 and 2016, respectively. He is the former Head of the Center of Intelligent and Autonomous Systems (CIAS) at university Tun Hussein Onn Malaysia (UTHM). He is currently the Chief Editor of the Journal of Soft Computing and Data Mining (JSCDM). Stanford University and Elsevier have selected him as one of the World's TOP 2% Scientists in 2021-2024. He has produced over 230 Scopus-indexed articles published in journals, books, and conference proceedings. His current H-index in Scopus is 40. He has completed 14 industrial projects and 23 research projects. His research interest is in Artificial Intelligence.

**Saraswathy Gunasekaran** is a senior lecturer at UNITEN, where she works on enriching the academic realm of her students through a fun and engaging classroom environment. Her research interest in the field of Artificial Intelligence has bagged her gold and silver awards in international competitions apart from actively engaging herself with potential industries to further commercialize her research ideas. She looks forward for collaboration possibilities in the areas of agent technology essentially in the field of social commerce and Smart Sustainable Cities. Currently, she is working on a Smart University Blueprint with IBM.